Accelerate Microsoft Office 365 Shared Deployments with Cisco WAAS WAN Optimization

What You Will Learn

Cisco® Wide Area Application Services (WAAS) empowers IT departments to provide a consistent user experience for core business applications across WAN links in branch offices and remote sites. The newest technology advancement in application access is the software-as-a-service (SaaS) model, in which applications are hosted in the cloud and delivered on demand to users. Microsoft Office 365 is a SaaS application option that allows IT departments to provide Microsoft Office productivity tools to employees.

This document focuses on the configuration steps needed to gain the optimization benefits that Cisco WAAS provides to Microsoft Office 365 shared deployments.

Cisco WAAS Overview

The cloud promises to deliver a range of benefits, including a shift from capital-intensive to operating-cost models, lower overall costs, greater agility, and reduced complexity. It also challenges enterprise IT departments in the way that they provide quality of service to employees while maintaining costs and manageability. Many organizations are seeking opportunities to migrate existing enterprise applications to a cloud system or an application infrastructure. Although this approach may provide benefits in that the application or system supports a distributed structure, IT teams are still going to be faced with user experience (performance) challenges along with access management and monitoring of these cloud-delivered solutions. Cisco WAAS offers the capability to address these challenges and deliver a consistent application experience to remote branch-office users. Figure 1 provides an overview of some typical Cisco WAAS deployment scenarios.

Figure 1. Cisco WAAS Enterprise Deployment
Microsoft Office 365 Services Overview

Whereas Microsoft Office is a collection of productivity software (including Microsoft Word, PowerPoint, Excel, Outlook, and OneNote) that is installed on the desktop or laptop computer, Microsoft Office 365 is an online subscription service that provides email, shared calendars, the capability to create and edit documents online, instant messaging, web conferencing, a public website for the business, and internal team sites - all accessible anywhere from nearly any device.

Customers with Microsoft Office 2010 or later installed on their computers can quickly configure their software to work with Microsoft Office 365. These users can easily retrieve, edit, and save Microsoft Office documents in the Microsoft Office 365 cloud, co-author documents in real time with others, and quickly initiate PC-to-PC calls and instant messages and web conferences with others.

SaaS applications typically are served from multiple SSL server farms, with multiple hosts spanning several data centers. For SSL services hosted in the enterprise data center, the IT administrator knows and controls the SSL server IP address and can provide it to the Cisco WAAS devices in the data center. But for an SSL service hosted at a third-party provider, the SSL server’s IP address is controlled by the SaaS provider. Moreover, there may be not just one but multiple servers or multiple IP addresses, even for a single SaaS service, and these addresses are subject to change. In addition, domain names used by the SaaS provider may periodically change, with new ones added and older ones removed. When domains are not updated in a timely manner for any SaaS application, errors due to namespace and certificate mismatch can occur.

Microsoft Office 365 Deployment

Microsoft Office 365 supports two deployment models:

- **Shared:** A Microsoft Office 365 shared deployment is a cloud-based service that is designed to help meet an organization’s needs. These services use a shared environment to host multiple customers. You can find more information about the offerings at [http://technet.microsoft.com/en-us/library/dn127064%28v=office.14%29.aspx](http://technet.microsoft.com/en-us/library/dn127064%28v=office.14%29.aspx).

- **Dedicated:** Microsoft Office 365 dedicated plans deliver cloud-based business services from Microsoft data center equipment that is dedicated to a company or organization and is not shared with any other organization. You can find more information about the dedicated service at [http://technet.microsoft.com/en-us/library/dn270088.aspx](http://technet.microsoft.com/en-us/library/dn270088.aspx).

Regardless of the deployment model, most communication between clients and servers is encrypted, requiring any WAN optimization or application acceleration technology in use to support the SSL encryption techniques being used.

**Note:** Some applications in the Microsoft Office 365 suite rely on federated services for authentication and authorization, and these services are outside the scope of this document.
Scope

This technical white paper discusses the use case in which client-to-cloud traffic is SSL encrypted and backhauled to the data center and then sent to the Microsoft Office 365 cloud, as illustrated in Figure 2.

Figure 2. Branch Internet Traffic Is Backhauled to Data Center and Then Sent to the Cloud

Essentially, you follow three steps to use Cisco WAAS to optimize Microsoft Office 365:

- Obtain the Microsoft Office 365 URLs and create an SSL certificate to optimize them.
- Create an SSL accelerated service for Microsoft Office 365 in Cisco WAAS and apply it to core devices.
- Use Cisco WAAS to accelerate Microsoft Office 365 shared traffic. Monitor the optimization levels and find out if any domains are missing from the original proxy certificate you created. Add any domain updates made by Microsoft to a new certificate and apply the certificate to the SSL accelerated service.

The following are prerequisites for using Cisco WAAS to optimize Microsoft Office 365 traffic:

- Cisco WAAS Software Release 5.3.5 installed and configured on the group of data center devices optimizing SSL-encrypted Microsoft Office 365 traffic. Cisco WAAS 5.3.5 introduces specific enhancements to handle the Microsoft Office 365 traffic.
- Cisco WAAS Central Manager (WCM) running Cisco WAAS Software Release 5.3.5 to support server name identification (SNI). SNI is an extension to the SSL and Transport Layer Security (SSL/TLS) protocol that indicates the hostname to which a client is attempting to connect at the start of the handshake. This protocol allows a server to present multiple certificates on the same IP address and port number, and hence allows multiple secure websites (or any other service over SSL/TLS) to be served from the same IP address without requiring all those sites to use the same certificate. It is the conceptual equivalent of HTTP/1.1 virtual hosting for HTTPS.
- An enterprise root certificate authority (CA) trusted by domain clients and computers. This CA needs to be capable of accepting certificate signing requests (CSRs) that include subject alternative names and generate certificates that include subject alternative names. The subject alternative name is an extension to the X.509 protocol that allows various values to be associated with a security certificate (SSL certificate). Subject alternative names can include IP addresses, email addresses, universal resource identifiers (URIs), alternative common Domain Name System (DNS) names, alternatives to the distinguished name, and other information.
First-Time Setup

Use the following steps to bring up a root CA. If your organization already a root CA for its internal use, you can use it instead of a new root CA.

Bring Up a Root Certificate Authority.
1. Follow the directions found in Microsoft’s TechNet article “Install a Root Certification Authority”. For more detailed information, refer to Microsoft’s TechNet article “Active Directory Certificate Services Step-by-Step Guide”.

2. Configure the web server certificate template. This template is used later to generate a proxy certificate for Cisco WAAS Central Manager. You will need to follow the directions found in Microsoft’s TechNet article “Configure the Web Server Certificate Template”.

3. Modify the CA to accept subject alternative names. By default, the Microsoft Windows root CA will not accept subject alternative names; therefore, you need to modify the registry to allow subject alternative names in the template created previously. To do so, follow Microsoft’s support article ID 931351, titled “How to Add a Subject Alternative Name to a Secure LDAP Certificate”. Follow only the first step (“How to Configure a CA to Accept a SAN Attribute from a Certificate Request”).

4. A self-signed root CA certificate is generated during the installation and configuration of the root CA. Microsoft Active Directory services will push this certificate to all Microsoft Windows clients in the domain (Microsoft Windows auto-enrollment). You can verify its existence on client machines by opening the Microsoft Management Console and adding the Certificates snap-in (Figure 3).

Figure 3. Adding the Certificates Snap-in
Make sure to select the computer account. Double-click Certificates (Local Computer), browse to Trusted Root Certification Authorities/Certificates (Figure 4). In the center pane, look for your root certificate. If the certificate is not present, you can push it using a global policy as described in the Microsoft TechNet note titled “Deploy Certificates by Using Group Policy”.

Figure 4. Verifying the Presence of a Root CA Certificate on Client Machines

5. For clients that are not integrated with Microsoft Windows Active Directory, such as Linux, Solaris, Mac OS, and mobile devices, you can install the root CA certificate manually in the browsers so these devices can benefit from the same optimizations as Microsoft Windows clients. To do so, follow the corresponding instructions for the different browsers (Mozilla, Safari, Chrome, etc.) to install an SSL certificate in a browser.

Provisioning and Operations

Now that the CA is up and operational and all clients requiring Microsoft Office 365 access have a root CA certificate installed, the next step is to configure Cisco WAAS to optimize the traffic using a proxy certificate. This certificate will specify a number of domains associated with Microsoft Office 365. For an up-to-date list, see the Microsoft TechNet article titled “Microsoft Office 365 URLs and IP Address Ranges”.

1. Generate a proxy (Cisco WAAS accelerated service) certificate. Using your CA, issue a certificate with the proper SANs, which can be found at the link listed in the preceding paragraph. Make sure to include all relevant links to your Microsoft Office 365 setup. A blog entry titled “Create Subject Alternative Name Certificate with Active Directory Certificate Services” is extremely useful. Make sure to install the newly created certificate on your Microsoft Windows system. By default, the new certificate will be placed under Console Root\Certificates - Current User\Personal\Certificates (shown later in Figure 6).
2. Export the proxy certificate. After this certificate has been generated and installed on the Microsoft Windows system, it needs to be exported and placed in a location from which it can be accessed when browsing to the Cisco WAAS Central Manager. All these steps must be done on the system from which the request was generated and the certificate was installed. To export the proxy certificate follow these steps:

   a. Open the Microsoft Management Console and add the Certificates snap-in (shown earlier in Figure 3). Make sure to select the My User Account button in the Certificates snap-in window (Figure 5).

   b. Find the certificate to export under Certificates - Current User\Personal\Certificates (Figure 6).

   c. Right-click the certificate and choose All Tasks > Export (Figure 6).

Figure 5. Select the My User Account Button

![Certiﬁcates snap-in](image)

Figure 6. Certiﬁcates - Current User\Personal\Certificate Contains the Certiﬁcate to Export

![Certificates - Current User\Personal\Certificate](image)
d. The Certificate Export Wizard launches. Click Next once. On the Export Private Key screen, select Yes, Export the Private Key (Figure 7) and click Next.

Figure 7. Export Private Key Window of the Certificate Export Wizard

![Certificate Export Wizard](image)

In the Export File Format window, select Personal Information Exchange - PKCS #12 (.PFX) and select both the first and third boxes (Figure 8). Then click Next.

Figure 8. In the Export File Format Window, Select Both the First and Third Boxes

![Certificate Export Wizard](image)
f. Provide a password and retype it. You will need this password later when you import the certificate into Cisco WAAS Central Manager. Click Next.

g. Select the path and name where the exported certificate is saved. Click Next.

h. The Completing the Certificate Export Wizard provides a summary of the export operation. You can verify it and then click the Finish button. If all went well, a window stating that the export was successful will appear, and the wizard will close.

3. Configure an SSL accelerated service in Cisco WAAS Central Manager.

a. Open a browser and connect to your Cisco WAAS Central Manager (https://wcm-ip-address:8443 or https://wcm-hostname:8443); see Figure 9.

Figure 9. Cisco WAAS Central Manager Login Screen

b. Create a device group for SSL services if you don’t have one already (Figure 10). You can choose to create a new group dedicated only to Microsoft Office 365 services.

Figure 10. Select or Create a Device Group for the SSL Accelerated Service
c. Assign the specific devices that will handle the SSL traffic. These devices reside in the data center and will optimize the SSL traffic as it passes through them on their way to the cloud. To do so, choose Device Groups and your device group name. Hover over the name and select Assign Devices (Figure 11). In this example, the device group name is SSL Services.

Figure 11. Select and Assign Devices to a Group

![Figure 11](image1.png)

d. Create an SSL accelerated service for the device group.
   i. Hover your mouse cursor over the Configure tab and choose Acceleration > SSL Accelerated Services (Figure 12).

Figure 12. On the Device Group Page, You Can Configure, Monitor, and Administer the Group Using the Tabs Next to the Group Name

![Figure 12](image2.png)
ii. Click the Create button (Figure 13).

Figure 13. Creating a New SSL Accelerated Service

iii. The Creating New SSL Accelerated Service page opens (Figure 14).

iv. In the SSL Accelerated Service section, as shown in Figure 14, name your service (1) and select both In Service and Match Server Name Indication boxes (2). You can also provide a short description.

Figure 14. Creating a New SSL Accelerated Service: SSL Accelerated Service Section

v. In the Server Addresses section, as shown in Figure 15, enter any in the IPAddress box (1) and 443 in the Server Port box (2). Then click Add (3).

Figure 15. Creating a New SSL Accelerated Service: Server Addresses Section
vi. In the Certificate and Private Key section, as shown in Figure 16, click Import Existing Certificate and Optionally Private Key (1), and select Upload File in PKCS#12 Format (2). Supply the password used to export the certificate (refer to step 2.f earlier in this section) (3). Using the Browse button (3), locate the certificate. Then click the Import button (4).

Figure 16. Creating a New SSL Accelerated Service: Certificate and Private Key Section

vii. A confirmation screen with the certificate information appears (Figure 17). Click the Submit button at the bottom of the page.

Figure 17. Certificate and Private Key Screen Showing the Imported Certificate Information
viii. The newly created SSL accelerated service is now displayed in the Cisco WAAS Central Manager (Figure 18).

**Figure 18.** List of All SSL Accelerated Services Configured for the Device Group

![List of All SSL Accelerated Services Configured for the Device Group](image1)

e. Verify that the accelerated service has been propagated to the device group members.
   i. Log on to the console of any of the devices assigned to the SSL accelerated service.
   ii. At the prompt, issue the `show crypto ssl services accelerated-service` command. Cisco WAAS should return the names of all accelerated services configured on the system, as shown in Figure 19.
   iii. Issuing the same command with the name of the service will provide more information about the accelerated service (see Figure 28 later in this section).

**Figure 19.** SSL Accelerated Services Present in Cisco WAAS and Their Status

![SSL Accelerated Services Present in Cisco WAAS and Their Status](image2)

4. Monitor Microsoft Office 365 optimization statistics using the Cisco WAAS Central Manager and the command-line interface (CLI). Because domain names can change without notice, it is a good practice to use Cisco WAAS to monitor whether other domains are being seen by Cisco WAAS but not matched by the certificate created earlier (refer to step 1 earlier in this section).
a. You can view optimization reports in the Cisco WAAS Central Manager.
   i. Beneath Devices > Device Name > Monitor > Optimization > Connections Statistics, each connection that is being optimized by the device is displayed (Figure 20).

**Figure 20.** Viewing Connection Statistics in Cisco WAAS Central Manager: First Three Connections Are Optimized by the SSL Accelerated Service Created to Optimize Microsoft Office 365 Traffic

ii. Each individual connection can be viewed for further details by selecting the magnifying glass icon to the left of Source IP:Port column. Figure 21 and Figure 22 show examples of the output data.

**Figure 21.** Inspecting Statistics for a Single Connection: Displayed Are Traffic Statistics (1), Amount of Time the Connection Has Been Open (2), Compression Rate (3), and Overall Summary (4)
b. Using CLI commands, you can determine which additional domain names may need to be added to the proxy certificate created earlier. This step allows the SSL accelerated service to be updated with any new domains that Microsoft may have added to the Microsoft Office 365 server content. The same information can be retrieved using the Cisco WAAS Central Manager GUI using the Show Commands option: from the device's dashboard, choose Monitor > CLI Commands > Show Commands, as shown in Figure 23. Figure 24 shows the output.

Figure 23. Using the GUI to Issue CLI Commands for a Single Device
c. Issuing the **show crypto certificates** command displays all the SSL certificates installed on the device (Figure 25). Notice that there are several stores, including Certificate Only Store, Managed Store, and Local Store. The focus is on Managed Store.

**Figure 25.** Displaying the Certificates of a Cisco WAAS Device
d. Issuing the `show crypto certificate-detail <certificate-name>.p12` command provides details of the certificate in the query. These details include the serial number, issuer, validity, and more, as shown in Figure 26.

**Figure 26.** Inspecting the Microsoft Office 365 Proxy Certificate Installed on a Cisco WAAS Device

```
show crypto certificate-detail Office-365.p12
```

![Certificate Details](image)

- **Bog Attributes**
  - **friendlyName**: 0
  - **localKeyId**: 85 28 42 0F E0 04 34 3A 5B 2C CF 1B A1 CA 74 F3 88 5C 28 28
- **Certificate**
  - **Version**: 3 (0x2)
  - **Serial Number**: 3B:1E:2B:00:00:00:00:11
  - **Signature Algorithm**: sha1WithRSAEncryption
  - **Issuer**: DC=local, DC=adbu, CN=ADBU-ROOT-CA
  - **Validity**
    - **Not Before**: Jan 23 22:21:53 2014 GMT
    - **Not After**: Jan 23 22:21:53 2016 GMT
  - **Subject**: CN=office365.com
  - **Subject Public Key Info**
    - **Public Key Algorithm**: rsaEncryption
    - **Public-Key**: (2048 bit)
    - **Modulus**: 00:06:6c:1f:fa:84:94:bc:5a:db:bd:cc:14:df:3d:

- **e.** Scrolling down in this command output, you can verify which SANs have been included, as shown in Figure 27.

**Figure 27.** Inspecting the SANs Included in the Certificate

```
X509v3 extensions:
1.3.6.1.4.1.327.4.
0.x.408.......
X509v3 Extended Key Usage:
TLS Web Server Authentication
X509v3 Key Usage:
Digital Signature, Key Encipherment
1.3.6.1.4.1.319.36:
0.0
X509v3 Subject Key Identifier:
X509v3 Subject Alternative Name:
DNS:*.live.com, DNS:*.microsoft.com, DNS:*.microsoftonline.com, DNS:*.mmsc.m功德.com, DNS:*.office.net, DNS:*.office365.com
X509v3 Authority Key Identifier:
```
f. Issue the `show crypto ssl services accelerated-service <service-name>` command (Figure 28) to display domains not included in the certificate created earlier. In the example, the SSL service is named Office-365. Again, the same information can be obtained from the device GUI as shown earlier in Figure 24.

**Figure 28. Verifying the Domain Names to Add to a New Certificate**

![Image of command output](image)

Following SNI servernames did not match the certificate

<table>
<thead>
<tr>
<th>Count</th>
<th>Last Seen</th>
<th>Servername</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>Dec 22 00:23</td>
<td>secure.addcdn.microsoftonline-p.com</td>
</tr>
<tr>
<td>2</td>
<td>Dec 22 00:25</td>
<td>portal.microsoftonline.com</td>
</tr>
<tr>
<td>1</td>
<td>Dec 22 00:25</td>
<td>xs1.outlook.com</td>
</tr>
<tr>
<td>8</td>
<td>Dec 22 00:26</td>
<td>login.microsoftonline.com</td>
</tr>
<tr>
<td>2</td>
<td>Dec 22 00:26</td>
<td>update.microsoft.com</td>
</tr>
<tr>
<td>9</td>
<td>Dec 22 00:30</td>
<td>outlook.office365.com</td>
</tr>
</tbody>
</table>

You will need to create a new certificate that includes all the domains specified in the original certificate created earlier in step 1 and any new domains that you believe should be optimized as reported by Cisco WAAS. Cisco does not recommend simply adding all domains without consideration.

h. After a new certificate is created, export the certificate (refer to step 2 earlier in this section) and install it as described in step 3.d.vi earlier.

**Note:** When issuing the new certificate (one that includes the new SANs), a staging process for the new certificate can be considered. Although the solution is expected to continue to optimize traffic even when new SANs are added, the cautious administrator can choose to stage the new certificate to a small set of users. If no problems are encountered, the certificate can be deployed to the whole enterprise. This process can be achieved by creating a stage-accelerated service (follow the directions in step 3 earlier in this section). This new service differs from the enterprise-wide accelerated service in that the new certificate is configured with a source IP address for a test client or small pool of clients. To limit the number of users, you can choose between implementing an interception access control list (ACL) or a Web Cache Communication Protocol (WCCP) redirection list. After verifying that there are no problems with the new certificate, you can push the certificate to the production service. Interception ACLs are a function of the Cisco WAAS device while WCCP redirection lists are a function of the router. You can find more information at these links:

- **Interception ACL:**

- **WCCP redirect-list:**
Solution Limitations

Microsoft Office 365 includes many components and applications. Microsoft Outlook has been fully tested and is known to work without any problems. Other applications are expected to work without any problems, too; however, this status can change over time, and you may encounter unknown problems.

This document covers only the optimization of Microsoft Office 365 when traffic is backhauled to the data center. Cisco WAAS does not support the optimization of a Microsoft Office 365 shared deployment when it is accessed directly from the Internet.

This document cannot guarantee that this solution will completely eliminate client-side certificate validation errors because there are certain browser plug-ins that validate certificates, such as HTTPS Everywhere, Perspectives, and Convergence.

For the Lync application, when logging in to Lync through the Microsoft Office 365 portal, the user will time out and will not be able to use Lync. To avoid this problem, be sure to exclude all Lync-specific domain names from the proxy certificate. This list includes *.lync.com.

For More Information

Read more about Cisco WAAS on the web or contact your local account representative.